Anomaly Detection Report

Model: autoencoder

Source File: orglog1.csv

Total Anomalies Found: 11

Anomaly #0 | Severity: High | Type: Data Exfiltration (Score: 2609.5681)

```
Log Details:
syslog_ts: Jan 28 09:00:00  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id:
12345  domain: abc.example.net  apache_ts: 28/Jan/2026:09:00:00 +0530  request: GET /utxLogin/login HTTP/1.1
status: 302  bytes: 249  response_time: 6  referer: -  user_agent: -
```

LLM Analysis:

The anomaly detected in the server log indicates potential data exfiltration activity, where sensitive information may have been extracted from the server.

Reason for Detection:

The unusually high status code (302), negative size, and negative duration values suggest abnormal behavior that could be indicative of data exfiltration attempts.

Anomaly #1 | Severity: High | Type: Data Exfiltration (Score: 2601.1201)

```
Log Details:
syslog_ts: Jan 28 09:00:00  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id:
12345  domain: abc.example.net  apache_ts: 28/Jan/2026:09:00:00 +0530  request: GET / HTTP/1.1  status: 302
bytes: -  response_time: 1  referer: -  user_agent: -
```

LLM Analysis:

The server log anomaly indicates potential data exfiltration activity, where sensitive information may have been extracted from the server.

Reason for Detection:

The unusually high status code (302), negative size value, and negative duration suggest abnormal data transfer behavior, which is indicative of data exfiltration.

Anomaly #2 | Severity: High | Type: Data Exfiltration (Score: 2601.0000)

```
Log Details:
syslog_ts: Jan 27 22:51:42  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id:
12345  domain: abc.example.net  apache_ts: 27/Jan/2026:22:51:42 +0530  request: GET / HTTP/1.1  status: 302
bytes: -  response_time: 0  referer: -  user_agent: Mozilla/5.0 (Windows NT; Windows NT 6.2; en-IN)
WindowsPowerShell/5.1.26100.7462
```

LLM Analysis:

The anomaly in the log features suggests potential data exfiltration activity, where the attacker may be attempting to steal sensitive information from the server.

Reason for Detection:

The unusually high status code (1768.6004) and negative values for size and duration indicate abnormal behavior that could be indicative of data exfiltration attempts.

Anomaly #3 | Severity: High | Type: Suspicious User Agent (Score: 2601.0000)

```
Log Details:
syslog_ts: Jan 27 22:51:52  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id: 12345  domain: abc.example.net  apache_ts: 27/Jan/2026:22:51:52 +0530  request: GET / HTTP/1.1  status: 302  bytes: -  response_time: 0  referer: -  user_agent: Mozilla/5.0 (Windows NT; Windows NT 6.2; en-US) WindowsPowerShell/5.1.26100.7462
```

LLM Analysis:

The anomaly detected in the server log indicates a potential attack involving a suspicious user agent.

Reason for Detection:

The anomaly features such as abnormal status code (1768.6004), negative size (-17.7480), and negative duration (-4.0463) point towards a potential malicious activity from a user agent with unusual behavior.

Anomaly #4 | Severity: High | Type: Data Exfiltration (Score: 2601.1201)

```
Log Details:
syslog_ts: Jan 27 22:51:52  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id: 12345  domain: abc.example.net  apache_ts: 27/Jan/2026:22:51:52 +0530  request: GET /utxHomeApp/redirectToHome HTTP/1.1  status: 302  bytes: -  response_time: 1  referer: -  user_agent: Mozilla/5.0 (Windows NT; Windows NT 6.2; en-US) WindowsPowerShell/5.1.26100.7462
```

LLM Analysis:

The anomaly in the log features such as unusually high status code, negative size, and negative duration indicate a potential data exfiltration attempt.

Reason for Detection:

The abnormal values in the status, size, and duration fields suggest that this log entry may be part of a data exfiltration attack where sensitive information is being extracted from the server.

Anomaly #5 | Severity: High | Type: Data Exfiltration (Score: 2601.0000)

```
Log Details:
syslog_ts: Jan 27 22:51:56  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id: 12345  domain: abc.example.net  apache_ts: 27/Jan/2026:22:51:56 +0530  request: GET / HTTP/1.1  status: 302  bytes: -  response_time: 0  referer: -  user_agent: Mozilla/5.0 (Windows NT; Windows NT 6.2; en-US) WindowsPowerShell/5.1.26100.7462
```

LLM Analysis:

The anomaly in the log features indicates potential data exfiltration activity, where sensitive data is being extracted from the server.

Reason for Detection:

The unusually high status code (302), negative size value, and negative response time suggest abnormal behavior that could be indicative of data exfiltration attempts.

Anomaly #6 | Severity: High | Type: Data Exfiltration (Score: 2601.1201)

```
Log Details:
syslog_ts: Jan 24 14:14:28  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id: 12345  domain: abc.example.net  apache_ts: 24/Jan/2026:14:14:28 +0530  request: GET /boardwebapp/company/ HTTP/1.1  status: 302  bytes: -  response_time: 1  referer: -  user_agent: curl/8.4.0
```

LLM Analysis:

The anomaly in the log details indicates potential data exfiltration activity where sensitive information may have been extracted from the server.

Reason for Detection:

The unusually high status code (302), negative size value, and negative duration suggest abnormal behavior that could be indicative *of data exfiltration attempts.*

Anomaly #7 | Severity: High | Type: Data Exfiltration (Score: 2601.1201)

```
Log Details:
syslog_ts: Jan 27 22:52:41  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id:
12345  domain: abc.example.net  apache_ts: 27/Jan/2026:22:52:41 +0530  request: GET /utxHomeApp/redirectToHome
HTTP/1.1  status: 302  bytes: -  response_time: 1  referer: -  user_agent: -
```

LLM Analysis:

The anomaly in the log features suggests potential data exfiltration activity, where sensitive information may have been transferred out of the system.

Reason for Detection:

The unusually high status code (302), negative size value, and negative duration indicate abnormal behavior consistent with data exfiltration attempts.

Anomaly #8 | Severity: High | Type: Suspicious User Agent (Score: 2602.7412)

```
Log Details:
syslog_ts: Jan 24 14:23:26  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id:
12345  domain: abc.example.net  apache_ts: 24/Jan/2026:14:23:26 +0530  request: GET /agmipad/ HTTP/1.1  status:
302  bytes: -  response_time: 13  referer: -  user_agent: curl/8.4.0
```

LLM Analysis:

The anomaly in the log details, specifically the user agent 'curl/8.4.0', indicates a potential malicious activity or unauthorized access attempt.

Reason for Detection:

The user agent 'curl/8.4.0' is not a common user agent for regular web browsing, suggesting a suspicious behavior that may require further investigation.

Anomaly #9 | Severity: High | Type: Directory Traversal (Score: 27.2270)

```
Log Details:
syslog_ts: Jan 28 12:52:40  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id:
559541  domain: projectcommercials-uat.test.company.net  apache_ts: 28/Jan/2026:12:52:39 +0530  request: GET
/pAccounting/appResources/js/angular/controller/fcm/fcmSupportController.js?v=/../../../../../../../../bin/id%0
0|  HTTP/1.1  status:  200  bytes:  2202  response_time:  1148  referer:
https://projectcommercials-uat.test.company.net/pAccounting/index.html  user_agent:  Mozilla/5.0  (Windows  NT
10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
```

LLM Analysis:

The anomaly in the log details indicates a potential Directory Traversal attack where the attacker is trying to access sensitive files by manipulating the file path in the request.

Reason for Detection:

The abnormal request 'GET /pAccounting/appResources/js/angular/controller/fcm/fcmSupportController.js?v=/../../../../../../../../bin/id%00|' with negative values in status and size, along with a suspiciously short response time, suggests an attempt to access system files outside the web root directory.

Anomaly #10 | Severity: High | Type: Path Traversal (Score: 12.4899)

```
Log Details:
syslog_ts: Jan 28 12:40:35  host: servernameabc  process: httpd[12345]  ip1: 0.0.0.0  ip2: 0.1.0.1  session_id:
```

Anomaly Detection Report

```
559541  domain: projectcommercials-uat.test.company.net  apache_ts: 28/Jan/2026:12:40:35 +0530  request: GET
/pAccounting/extResources/tooltip/tipsy-docs.js?v=/../..//../..//../..//../..//../..//../..//..///etc/passwd%00
HTTP/1.1  status: 200  bytes: 931  response_time: 5  referer:
https://projectcommercials-uat.test.company.net/pAccounting/index.html  user_agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
```

LLM Analysis:

Likely Path Traversal attack based on the abnormal request path that attempts to access sensitive system files.

Reason for Detection:

The anomaly in the request path with multiple '../' indicates an attempt to traverse directories and access system files, such as the '/etc/passwd' file, which is a common tactic in Path Traversal attacks.